Aging and Disability Resource Center
POLICIES AND PROCEDURES

TOPIC:	Confidentiality
EFFECTIVE DATE:	
REVISION DATE:	

DRAFT

Model ADRC Confidentiality Policy and Procedures

1.0 Policy

The ADRC shall respect the privacy of its customers and ensure the confidentiality of its customers' personal information.

2.0 Purpose

The purpose of this policy is to provide guidance on how information should be accessed or shared consistent with the customer's right to privacy and respect and with the requirements of state and federal law. These policies and procedures are in addition to and do not replace any county confidentiality policy(ies) that apply to the ADRC.

3.0 Applicability and Responsibility for Compliance

All ADRC staff, including volunteers and contractors, are expected to be familiar and comply with the requirements of this confidentiality policy. Benefit Specialists are subject to the confidentiality requirements specific to their program and should follow their program guidelines when different from this more general policy (e.g., reporting abuse and neglect and sharing information with MCOs).

4.0 Staff Training and Assurances

All newly hired ADRC staff will be trained on the confidentiality policy as part of their orientation, and refresher training will be conducted on an annual basis.

All ADRC staff must sign a confidentiality and non-disclosure agreement stating that they have reviewed, understand and will abide by the confidentiality policy before being given access to confidential customer information. A copy of the policy is given to each staff member for their records and a copy of the signed confidentiality agreement is kept in the staff member's personnel file. This agreement shall be reviewed and signed annually, at the time when a performance evaluation is completed.

5.0 Types of Client Information that are Considered Confidential

Any personal information about an ADRC customer is considered confidential, including but not limited to:

- The person's name, address, birth date, Social Security number or other information that could be used to identify the individual
- The person's physical or mental health, functional status or condition
- Any care or services that the individual has or will receive from the ADRC or any other provider
- Financial information, including income, bank accounts and other assets, receipt of benefits, eligibility for public programs, method of payment for services provided to the individual, etc.
- Employment status or history
- Education records
- Any other information about the individual that may be obtained by ADRC staff

6.0 Who Has Access to Confidential Customer Information

ADRC staff may access confidential customer information in order to provide information and assistance, options counseling, benefits counseling, functional eligibility determination, enrollment counseling, and other ADRC services. ADRC supervisors may also have access to confidential information on an as needed basis.

7.0 Guidelines for Ensuring Confidentiality

7.1 Underlying Principles

Customer information should be handled consistent with the following principles:

7.1.1 Respect for the Privacy and Best Interest of the Customer Decisions about what customer information is to be accessed and/or shared shall be based on what is in the best interest of the customer consistent with the customer's right to privacy and respect. Customers should not be pressured to reveal more than they are willing to share and shall be allowed to remain anonymous if they so desire. Treat the customer's information as you would treat your own.

7.1.2 Informed Consent

Customers should be told that the information they share with the ADRC is kept in confidence and may be shared, when needed, with the customer's permission. It is best practice to inform customers about how their information will be used and to obtain at least a verbal consent, even if not strictly required.

If ADRC staff have reason to believe that the information the customer has shared or is about to share would not be protected, they should inform the customer of the limits to confidentiality. These include reporting abuse or neglect; cooperating with public health, adult protective services, law enforcement or a court order; and emergency situations (See Section 9.3 of this policy).

7.1.3 "Need to Know" and "Minimum Necessary" Standard

ADRC staff shall obtain only that information which they need to know in order to assist the customer and shall use customer information only for purposes directly related to the provision of ADRC services to the customer.

7.1.4 Compliance with Confidentiality Laws and Policies

Client confidentiality is protected by federal and state statutes and regulations and by county government policies and procedures. The ADRC and its staff will abide by all legal requirements relating to confidentiality.

7.2 Staff Actions to Safeguard the Confidentiality of Customer Information

ADRC staff are expected to employ the following practices in order to safeguard their customer's confidentiality:

- Only access personal and identifiable customer information when you need it in order to perform your job.
- Disclose confidential information only to those who need it to complete their tasks and are authorized to receive it.
- Obtain informed consent prior to accessing or disclosing information consistent with provisions of Sections 8 and 9 of this policy.
- Discuss a customer's information with his/her friends, family members, visitors, or anyone else not permitted access to such information only when the customer so wishes and agrees.
- Do not access information about your family members, neighbors or friends. Review any requests to serve people you know with your supervisor.
- Refrain from communicating information about a customer in a manner that would allow others to overhear.
    - Close the door or take customers to a private location before discussing confidential matters.
    - Avoid discussing customer information in an open area -- in the reception area, in the hall, in an elevator, by the copy machine, in a restaurant or other public place.
    - When it is necessary to discuss information in an open area, talk in a quiet voice and keep identifying information to a minimum.
- Keep confidential information out of sight.
    - Do not leave paperwork with confidential information in sight on your desk or work space, even at night.
    - Never leave paperwork unattended in common areas
    - Use a computer "privacy screen" if your work station is potentially visible to customers
- Protect access to electronic data.
    - External e-mails containing confidential customer information should be encrypted. External emails that are not secure should not contain any identifiable information.

  - Lock your computer when it is left unattended. This can be done by pressing CTRL/ALT/DEL.
  - Never leave your laptop unattended or in an unlocked car. When leaving a laptop in a locked vehicle, be sure it is out of sight and encrypted.
  - Do not disclose your user name and password, except in extenuating circumstances such an unanticipated medical leave.
  - Do not permit others to access the ADRC's computer system or network using your password or user ID code. Do not use another employee's password or user ID to access information.
- Fax transmissions that contain confidential information should be sent with a cover sheet that includes a confidentiality statement.
- Delete or dispose of information that is outdated and no longer needed.
  - Use a confidential recycling bin to dispose of written material that contains any identifiable customer information.
  - In disposing of electronic confidential information, wipe or destroy the information to render it unusable, unreadable or indecipherable. Deleting files is not sufficient. Contact your ADRC or county security officer if you are unsure how to do this.
- Report any violations of confidentiality to your supervisor.
- If unsure whether information may be disclosed, check with your supervisor.

7.3 ADRC Measures to Safeguard the Privacy of Customer Records and Data

In addition to the above guidelines for staff, the ADRC has the following safeguards in place to protect the privacy of records and data and to prevent inappropriate use or disclosure of client information:

- Locked file cabinets for confidential information and a secure area for records storage are provided.
- Documents that are no longer needed are shredded.
- ADRC computers are equipped with security features to protect client data from unauthorized interception, modification, or access during electronic transmission and receipt, transfer and removal of electronic media.
- Computers, laptops and portable devices have encryption software installed.
- When disposing of printers, copiers, scanners and fax machines, the hard drives are wiped or otherwise disposed of in a way that prevents access to captured document images.
- Staff who leave their employment or affiliation with the ADRC lose their ability to access client information and data systems, effective immediately upon their departure.

8.0 Accessing Records From Outside of the ADRC

ADRC customers or their guardians/ legal representatives shall be asked to sign a release of information form to permit the ADRC to access any confidential records it needs to complete the long term care functional screen or provide other ADRC services to the

individual. Signed forms shall be kept in the client's file and a copy of the signed form shall be provided to the individual.

9.0 Disclosure of Client Information

9.1 Disclosure of Client Status

Staff may not disclose or acknowledge whether a person has received or is receiving services from the ADRC, unless it has been established that the information can be legitimately shared. When unsure, staff receiving an inquiry regarding the status of a customer shall respond in a non-committal manner. For example, staff may say, "The ADRC confidentiality policy does not permit the disclosure of that information."

9.2 When Informed Consent is Required

Some situations require prior consent before releasing confidential customer information and others do not.

9.2.1 Disclosures That Require Prior Written Informed Consent

The types of disclosures that require prior signed authorization from the customer or the customer's legal representative include:

- Sharing information with counties outside of the ADRC service area
- Transfer of the long term care functional screen for any purpose other than enrollment into a Managed Care Organization (MCO) or IRIS.
- Sharing of medical information with an employer, life insurer, bank, marketing firm, news reporter or with any other external entity for purposes not related to the customer's care.
- AODA treatment records
- School records
- Any disclosure for purposes not relating to the services provided by the ADRC

Information obtained by ADRC from a third party such as a doctor's office, school, or AODA program may be redisclosed without an additional release if the release obtained by the original provider of the information included a statement authorizing redisclosure.

9.2.2 Process for Obtaining Written Informed Consent

The ADRC will obtain a signed release of information form that describes the information to be shared, who can use the information and is signed and dated by the customer whose information is to be shared or his/her legal representative. A copy of the signed release form shall be given to the customer or his/her the legal representative.

The records obtained and a copy of the signed release of information form shall be kept in the individual's file.

Any written disclosure of confidential information by ADRC staff shall be accompanied by a written statement documenting that the information is confidential and further disclosure without the individual's consent or statutory authorization is prohibited by law.

9.2.3 When Verbal Consent is Sufficient

The following situations require only verbal consent in order to share customer information:

- Sharing information with the individual's family, friends, caregivers and providers who are involved with the person's care when necessary to coordinate services for the individual.
- Contacting an agency or service provider on the customer's behalf.
- Referring the individual to services provided by the ADRC or other county departments or agencies.
- Linking customers to community resources.

Records of verbal consents should be documented and kept in the customer's file.

9.2.4 Customer Right to Revoke Consent

A written release of information or oral consent may be rescinded by the customer or his/her legal representative at any time. This should be done in writing, if possible. Revocation of a prior consent should be documented in the customer's file.

9.3 Disclosures Which May be Made Without Either Written or Verbal Informed Consent

9.3.1 Intra- and Inter-Agency and Interagency Disclosure

Neither written nor verbal informed consent is required in the following situations; however it is advisable to let the customer know that these exchanges may take place.

- The exchange of customer information is necessary for the ADRC to perform its duties or coordinate the delivery of services to the customer.
- Transferring the long term care function screen for the purpose of enrollment into a Managed Care Organization (MCO) or IRIS in the ADRC's service area.
- The exchange of information is necessary to coordinate the delivery of ADRC, county human services, social services, or community programs to the customer.

9.3.2 Other Disclosures Permitted Without Consent

The ADRC may share customer information and records without the individual's written or oral consent in the following circumstances:

i. In order to report possible abuse or neglect of an elderly person or vulnerable adult, per Wis. Stat. 46.90 and 55.043
ii. In order to cooperate with public health, adult protective services, elder/adult-at-risk investigations
iii. In order to cooperate with a law enforcement investigation
iv. As needed in the event of an emergency, per established emergency procedures
v. When the exchange of information is necessary for the Wisconsin Department of Health Services to administer the Family Care, IRIS, or Medicaid programs or to comply with statutorily-required advocacy services for Family Care enrollees and prospective enrollees
vi. Pursuant to a court order.

10.0 Informing Customers of Their Rights and Responding to Customer Requests

10.1 Informing Customers About the Confidentiality Policy

As a common practice, staff will ask customers whether they have any objection to sharing information, even if written authorization is not required. Staff will inform customers about the ADRC's confidentiality policy and the customer's right to see their records, obtain copies, and contest the information contained in those records.

10.2 Customer Requests to View or Get Copies of Their Records

ADRC customers have a right to view and/or receive copies of their records on file at the ADRC. To do so, the customer or his/her legal representative shall submit a written request, a copy of which will be kept in the customer's file, together with a record of what information was disclosed. Charges for paper copies may be required for copies of records exceeding 10 pages.

10.3 Requests to Share ADRC Information With a Third Party

If the customer wants information from his/her ADRC records given to a third party, the customer or his/her legal representative must complete a Release of Information form indicating which information is to be sent and to whom. Charges for requested paper copies may be required for copies that exceed 10 pages.

11.0 Monitoring and Ensuring Compliance

11.1 Responsibility for Monitoring and Compliance.

ADRC supervisors are responsible for monitoring and ensuring compliance with this confidentiality policy by conducting periodic compliance checks, reviewing the confidentiality policy with employees during performance evaluations, and providing training to staff.

11.2 Reporting Security Violations and Breaches of Client Confidentiality

ADRC staff shall report any breach of customer confidentiality to their supervisor as soon as it is discovered and follow the designated incident reporting process, where applicable.

11.3 Mitigating and Correcting Breaches of Confidentiality

Violations of the confidentiality policy will be documented and corrected. Where required or appropriate, consumers will be notified of the breach and of actions taken to mitigate the situation.

12.0 References

12.1 Confidentiality Policy(ies) of county(ies) in the ADRC service area

12.2 Wisconsin state confidentiality statutes and regulations

- Statutory requirements on ADRC confidentiality and sharing information: Wis. Stat. 46.283(7).
- Administrative rule standards for performance by resource centers: DHS 10.23(7) for ADRCs and DHS 10.23(2)(d)2 for the DBS

12.3 ADRC Contract, Exhibit I, Article IV. L. 1-6

http://www.dhs.wisconsin.gov/adrc/pros/index.htm

12.4 EBS and DBS Program Guidelines

- EBS confidentiality policy is outlined in Chapter 9.11.6 of the *Manual of Policies and Procedures and Technical Assistance for Wisconsin Aging Network*: http://www.dhs.wisconsin.gov/publications/P2/p23203.pdf
- **DBS Program Policies and Procedures: https://www.dhs.wisconsin.gov/adrc/pros/dbsppmanual.pdf**

12.5 HIPAA Privacy Rule

Note: The Wisconsin Department of Health Services (DHS) does not consider ADRCs to be a covered entity or business associate under HIPAA. The decision about whether the ADRC is subject to HIPAA privacy requirements is at the discretion of the county or ADRC's corporation counsel. If the county considers the ADRC to be subject to HIPAA, additional provisions to comply with HIPAA requirements should be included in the privacy policy. See http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html